REMARKS

The application is believed to be in condition for allowance.

Formal Matters

Claims 16-35 were rejected as indefinite.

Claims 16-35 were rejected as being incomplete for omitting essential steps.

Each of these two rejections are based on the recitations of the invention data sale immediate settling method executing an action chain including validating the prepaid card by comparing a user-input password number, input by the user, with a current password number stored in the database. The Official Action does not object to this portion of the claims.

However, the Official Action objects to the wherein clause which recites that (e.g., claim 16), asking how "a different user-input password number and a different current password number is required for each of plural transactions". This condition was explained in the following wherein clauses.

Initially, a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number. Then, after each validation, the user sets a new user-set password number as the current password number stored in the database. Thus, there is a different current password number stored in the database than was previously stored in the database.

As a result of the current password number stored in the database being different from the previously stored "current password number", the next validation requires a successful comparison of a user-input password number, currently input by the user, to the stored current password number.

Reference is made to specification page 2, beginning at line 7, wherein it is disclosed that the invention provides a data sale immediate settling method that includes actions on a purchaser's end of inputting the purchaser's ID, the n-th action of inputting the n-th password used at the n-th time to a terminal, an action of inputting the (n+1)-th password used at the (n+1)-th time to the terminal, and an action of inputting contents to the terminal. Actions on a seller's end include an action of distributing the contents to the purchaser, and an action of subtracting a price corresponding to the contents from the balance in a database. Beginning at line 17, it is explicitly disclosed that the password is changeable and that the password can be changed every time a purchase is implemented so that a security is significantly raised.

Beginning at line 24, it is disclosed that actions on the purchaser's end further include an action of re-inputting the (n+1)-th password used at the (n+1)-th time, and the action on the seller's end is to collate an agreement between the (n+1)-th password and the re-inputted (n+1)-th password. Then, the changed passwords are commonly confirmed on the purchaser's end

and the seller's end. The action on the seller's end is to register the (n+1)-th password on the basis of the collation of the agreement.

Reference is next made to the DESCRIPTION OF THE PREFERRED EMBODIMENT section of the specification, as well as the drawing figures.

See page 6, beginning with line 5 disclosing that in an embodiment with the real (physical) prepaid card, a serial number, a first-time password number, and an expiration date are visibly printed. As shown in Figure 1, there are registered to the database a serial number (100001), a first-time password number (36736492), a user set password number (blank), a card face value (3000), the balance (3000), etc. that all have a one-to-one correspondence with those of the specified prepaid card.

Figures 2-3 (beginning at line 26, page 6) illustrate the invention's method steps. Actions 1-4 relate to inputting the card's serial number and confirming that the card is usable. Actions 5-8 relate to the user input the initial password number and confirmation of whether or not the user-input password number has a one-to-one correspondence with the serial number to the database in order to allow the user further access.

Action 9 discloses the portal site requesting the user to input the password number used at the next time. Actions 10-16 are the user inputting and confirming the next-time

password number used for the access at the next time, and the next-time password being stored in the database.

Actions 16-32 relate to the user's transaction and updating the balance on the card. Actions 33-34 relate to ending the transaction and closing the link to the database. Action 35 is the portal site returning to the input waiting for the serial number of the card.

Returning to prior claim 16, the above passages and figures disclose 1) providing a user with a prepaid card linked to a database; and 2) executing an action chain including validating the prepaid card by comparing a user-input password number, input by the user, with a current password number stored in the database. There was also disclosed that 1) a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number, 2) after each validation, the user sets a new user-set password number as the current password number stored in the database.

As summarized on specification page 11, beginning with line 6, in this manner, the password number is changed every time of use so that the higher security is sustained. It is unnecessary to certify information related to an individual such as a credit card number, bank account number, address, or name when the card is used. Therefore, the card can be a gift or be used for a promotion of a company. By recording a kind, date,

and volume of the transacted contents on the database of the password number and the serial number of the card, information used for market research can be collected.

Claim 16 has been amended to clarify the recitations of the invention. Claim 16 now recites by step B) executing a first action chain including i) the user inputting a password number, ii) a first validation by comparing the user-input password number to a system-set first-time password number stored on the database as the current password number, and iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new user-set next-time password number.

Claim 16 also recites, by step C), executing another action chain including i) the user inputting another password number, ii) validation by comparison of the another password number to the stored new user-set next-time password number, and iii) the user entering another next-time password number and storing the another next-time password in the database as the new user-set next-time password number required for validation of the prepaid card in a next another action chain.

The wherein clause recites that step C) is repeated.

Also note that the next-time password is input prior to accessing the monetary balance on the card (Actions 17 et seq.).

Independent claim 30 has been similarly amended.

Withdrawal of the Section 112 rejections is therefore solicited.

Substantive Matters

Although the text of the Official Action indicates rejection of claims 16-21 and 30-35 (page 3), it is clear that all of claims 16-35 were rejected as obvious over KWAN 2003/0200179 in view of NOVOA 6,636,973; and claims 22-29 as obvious in further view of KHELLO WO 97/11443.

Applicant respectfully disagrees.

Although user inputting new passwords is known, the applied art teaches that it is more desirable to automate the changing of passwords, thereby avoiding requiring the user inputting new passwords each time an account/card is accessed.

Neither of KWAN nor NOVOA teaches the present invention's concept of having a user-supplied password set as part of each card validation and prior to accessing the card's monetary balance.

This approach provides both a convenient and elegant solution not taught or suggested by the applied art.

KWAN takes an opposite approach to that of the invention; that is, KWAN uses the system to set each next password number, e.g., codes are set by the merchant and the customer must accept the merchant-set code and later re-input the merchant-set code in order to validate the prepaid card.

The Official Action offers NOVOA for teaching that, after each of plural password validations, the user sets a new password number as the current password number stored in the database. The Official Action refers to NOVOA Abstract, column 2, lines 27-49; and column 3, lines 6-25.

This is incorrect. Column 2, lines 35-39 refers to prior art to NOVOA and not to the NOVOA system. In NOVOA, the password may be changed, but not by the user.

At some point during or after the log on process, the biometrics account manager changes the current password associated with the user to a new password and overwrites the previous password with the new password.

There is no disclosure in the Abstract of the concept of the user resetting the password after each existing password validation.

Indeed, see in column 3, lines 6-25 it is disclosed by NOVOA that beginning at line 15 (emphasis added) "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current password associated with the use to a new password. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security." If the user is not required to remember the password, it is clear that the user need not enter the new

password at a later time. This passage explicitly states that the user does not type the password.

See column 3, lines 26-30 stating that the password is generated randomly. See also column 9, lines 2-9. The new password is used to log on the user; however, the user does not enter the new password. The user does not select or enter the next-time password into the system during the current password validation.

Thus, each of these references teaches completely opposite to the recited invention where, the invention provides that the user inputs a new next-time password after entering and verifying the current password.

In the sentence spanning pages 4-5 of the Official Action, it is stated that KHELLO discloses to provide a higher user authentication service, and page 2, lines 26 to page 3, line 9 is offered.

In the offered passage, KHELLO is discussing prior art to KHELLO. In KHELLO's prior art is was known to improve security by 1) making access codes longer, 2) providing users with plural PIN codes to be entered in sequence, 3) requiring the user to change his PIN code each time a service is requested, and 4) using a scrambling terminal.

KHELLO teaches away from these approaches. KHELLO is critical of each of these alternatives and presents a different security improvement. Thus, although KHELLO teaches that one way

of improving security was requiring the user to change his PIN code each time a service is requested; however, KHELLO points out that this approach has drawbacks and suggests an alternative approach. KHELLO thus teaches away from the recited invention.

Further, KHELLO does not disclose any details as to how or when the user would be required to change his PIN code.

Each of the three applied references teaches increased complexity approaches to increased security, without the user entering a new password. One of skill would not be motivated to modify KWAN in the manner being urged by the Official Action.

Recall, the test is not whether the prior art included the necessary knowledge to make it possible to modify KWAN to achieve the presently claimed invention, but rather the test is whether there is motivation to modify KWAN to achieve the presently claimed invention.

The present rejection arises from improperly application of hindsight. Again, the analysis is not whether the prior art had the technology to achieve the invention, but rather the invention is taught or suggested by the relevant prior art.

Numerous Federal Circuit decisions emphasize that obviousness rejections over a combination of elements found in two or more prior art references are improper unless the prior art suggests their a combination. *E.g. McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001) (" 'the central question is whether there is reason to

combine [the] references,' a question of fact drawing on the *Graham* factors"); *In re Kotzab*, 208 F.3d 1365, 1370, 54 USPQ2d 1308, 1316 (Fed. Cir. 2000) ("to establish obviousness based on a combination of the elements disclosed in the prior art, there must be some motivation, suggestion or teaching of the desirability of making the specific combination that was made by the applicant.").

In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999) ("Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is a rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references.") ("The range of sources available [to show a suggestion, teaching, or motivation to combine], however, does not diminish the requirement for actual evidence. That is, the showing must be clear and particular."

"When the incentive to combine the teachings of the references is not readily apparent, it is the duty of the examiner to explain why of the reference teachings are proper." *Ex parte Skinner*, 2 USPQ2d 1788, 1790 (Bd. App. & Int'f 1986), *see also Ex parte* Clapp, 277 USPQ 972, 973 (Bd. App. & Int'f 1985) (noting that, to support obviousness, "either the references must expressly or impliedly suggest the claimed combination or the examiner must present a convincing line or reasoning as to why the artisan would have found the claimed

invention to have been obvious in light of the teachings of the references. . . . [S]implicity and hindsight are not proper criteria for resolving the issue of obviousness.")

For a prepaid card linked to a database, the applied art does not teach or suggest executing a first action chain for immediately settling a data sale which includes sequentially i) the user inputting a password number, ii) a first validation of the prepaid card by comparing the user-input password number to a system-set first-time password number stored on the database as the current password number, and iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new, user-set next-time password number, and iv) requesting a current monetary balance available on the prepaid card.

Nor do the references teach repeatedly executing further action chains including sequentially i) the user inputting another password number, ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password number, iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain, and then iv) requesting another current monetary balance available on the prepaid card.

Applicant is not arguing that individual parts of the claimed invention were not in the prior art. Rather, the combination of recited features is non-obvious, taking into account what the references actually teach.

First, the proposed combination of references disregards the claimed invention as a whole, and therefore should be withdrawn.

The Federal Circuit has held that in determining the differences between the prior art and the claims, the question under 35 USC 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983).

Any motivation to modify KWAN to satisfy the present claims is merely hindsight with the present disclosure being used to render the claimed invention obvious. Such an approach is not permitted.

The Federal Circuit emphasized in July, 1998 that "[m]ost, if not all, inventions are combinations and mostly of old elements." *In re Rouffett*, 47 USPQ 2d 1453, 1457 citing to *Richdel, Inc. v. Sunspool Corp.*, 219 USPQ 8, 12 (Fed. Cir. 1983). The Federal Circuit continued by noting that "rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a

blue print for piecing together elements in the prior art to defeat the patentability of the claimed invention."

Thus, the Federal Circuit requires that in order to prevent the use of such hindsight, the Official Action must "show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed." (*In re Rouffett* at 1458). The present rejection fails to meet this requirement.

The obviousness rejection is not viable.

Additionally, even if combined, the references would not teach the sequence of steps, as recited (validate old password, set new password, then check money of card).

In view of the above, reconsideration and allowance of all the claims are respectfully requested.

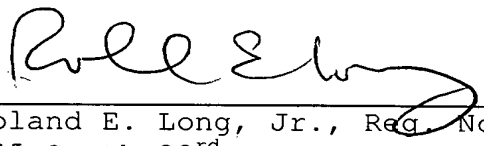
Applicant believes that the present application is in condition for allowance and an early indication of the same is respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lk